aws

建立防护栏并监控预签名 URL

AWS 规范性指导

AWS 规范性指导: 建立防护栏并监控预签名 URL

Table of Contents

为预签名者建立护栏并进行监控 URLs

Ryan Baker，亚马逊 Web Services (AWS)

2025 年 8 月（文档历史记录）

安全是所有公司最关心的问题，也是 AWS Well-Architected Framework 的关键支柱。作为一名安全工程师，你需要实施符合组织控制要求的管理护栏。在 Well-A AWS rchitected Framework 中，护栏定义了限制活动的边界。

本指南提供了使用预签名的背景信息和最佳实践 URLs，这些信息与亚马逊简单存储服务 (Amazon S3) Simple Service 对象一起使用。Presigned URLs 允许有权访问有效凭证的用户或应用程序生成预先签名的请求，并在定义的到期时间之前被接受。presigned 的一个常见用例 URLs 是通过共享这些请求来扩展对对象或资源的访问权限。共享的预签名请求由有权执行特定请求的系统或用户生成，然后可以发送给其他系统或用户以扩展执行相同请求的能力。

在本指南中，您将学习：

- 预签名的概念 URLs
- 预签名的用例 URLs
- 推荐和可选的护栏
- 监控选项
- 如何 AWS 服务 使用预签名的示例 URLs

目标受众

本指南适用于负责在 AWS 云中实施安全控制的架构师和安全工程师。

目标

作为一名安全工程师，你需要了解解决方案构建者是如何实现安全性的，以及最终用户拥有的访问权限类型。本指南涵盖了一种预签 URLs名访问类型，通常用于 Amazon S3。Presig URLs ned 为构建者提供了有效桥接身份验证机制的选项。

在 Amazon S3 中，预签名 URLs 代表一种独特的请求类别。安全工程师可以监控和管理这些请求，以确保仅在适当和必要的情况下使用这些请求。本指南的目的是帮助安全工程师提供此类高级监督。

阅读本指南后，您应该了解什么是预签名 URL，通常何时使用它，以及使用它的动机。

先决条件

如果您的公司尚未按照《在 AWS 上实施安全控制》指南中所述定义安全策略、控制目标或标准，我们建议您在继续阅读本指南之前完成这些监管任务。

在开始之前，您还应该熟悉控制和监控方面的推荐和可选最佳实践。有关更多信息，请参阅:

- 服务控制策略（AWS Organizations 文档）
- 资源控制政策（AWS Organizations 文档）
- 亚马逊 S3 的存储桶策略（亚马逊 S3 文档）
- 使用服务器访问日志记录请求（Amazon S3 文档）
- 使用 AWS CloudTrail（亚马逊 S3 文档）记录亚马逊 S3 API 调用

预签名概述 URLs

预签名网址是一种由 AWS Identity and Access Management (IAM) 服务识别的 HTTP 请求。这种类型的请求与所有其他 AWS 请求的区别在于X-Amz-Expires 查询参数。与其他经过身份验证的请求一样，预签名 URL 请求也包含签名。对于预签名 URL 请求，此签名将传入。`X-Amz-Signature`签名使用签名版本 4 加密操作对所有其他请求参数进行编码。

> **注意**
>
> - Signature 版本 2 目前正在被弃用，但某些 AWS 区域版本仍支持该版本。本指南适用于签名版本 4 签名。
> - 接收服务可以处理未签名的标头，但根据最佳实践，对该选项的支持有限且有针对性。除非另有说明，否则假设所有标头都必须经过签名才能被接受。

该`X-Amz-Expires`参数允许将签名视为有效，但与编码的日期时间偏差更大。 签名有效性的其他方面仍在评估中。 签名凭证（如果是临时证书）在处理签名时不得过期。 签名证书必须附加到在处理时拥有足够授权的 IAM 委托人。

预签名 URLs 是预签名请求的子集

预签名 URL 并不是将来签署请求的唯一方法。Amazon S3 还支持 POST 请求，这些请求通常也是预签名的。 预签名的 POST 签名允许上传符合已签名政策且该政策中包含有效期的上传。

请求的签名可能是 future 日期，尽管这种情况并不常见。 只要底层凭证有效，签名算法就不会禁止将来的约会。 但是，这些请求要等到有效的计时窗口才能成功处理，这使得对于大多数用例来说，future dating 是不切实际的。

预签名请求允许什么？

预签名的请求只能允许用于签署请求的凭据所允许的操作。如果凭证隐式或显式拒绝预签名请求指定的操作，则预签名请求在发送时将被拒绝。这适用于以下情况：

- 与凭证关联的会话策略
- 与与证书关联的委托人关联的基于身份的策略
- 影响会话或委托人的资源策略
- 影响会话或主体的服务控制策略
- 影响会话或委托人的资源控制策略

使用预签名请求的动机

作为一名安全工程师，你应该了解是什么促使解决方案构建者使用预 URLs签名。 了解什么是必要的，哪些是可选的，将有助于你与解决方案构建者沟通。动机可能包括以下几点：

- 支持非 IAM 身份验证机制，同时受益于 Amazon S3 的可扩展性。核心动机是直接与 Amazon S3 通信，以便从该服务提供的内置可扩展性中受益。如果没有这种直接通信，解决方案就需要支持重新传输传入的字节PutObject和GetObject调用的负载。根据总负载，此要求增加了解决方案构建者可能希望避免的扩展挑战。

  其他直接与 Amazon S3 通信的方式，例如在 AWS Security Token Service (AWS STS) 中使用临时凭证或在外部使用签名版本 4 签名 URLs，可能不适合您的用例。Amazon S3 通过 AWS 证书识别用户，而预签名的请求则假定通过证书以外的 AWS 机制进行身份识别。通过预签名的请求，可以弥合这种差异，同时保持数据的直接通信。
- 从浏览器的原生理解中受益 URLs. URLs 浏览器可以理解，而 AWS STS 凭据和签名版本 4 的签名却无法理解。这在与基于浏览器的解决方案集成时非常有用。替代解决方案需要更多的代码，将占用更多内存来存储大文件，恶意软件和病毒扫描程序等扩展程序可能会以不同的方式对待。

与临时 AWS STS 证书的比较

临时证书与预签名请求类似。 它们都过期，允许限制访问范围，并且通常用于将非 IAM 证书与需要 AWS 证书的使用联系起来。

您可以将临时 AWS STS 凭证的范围严格限定为单个 S3 对象和操作，但由于 AWS STS APIs 存在限制，这可能会导致扩展方面的挑战。（有关更多信息，请参阅 AWS re: Post AWS STS网站上的 “如何解决 IAM 的 API 限制或 “超出速率” 错误的文章。）此外，生成的每个凭证都需要一个 AWS STS API 调用，这会增加延迟和可能影响弹性的新依赖关系。 临时 AWS STS 凭证的最短到期时间也为 15 分钟，而预签名的请求可以支持更短的持续时间。（如果条件合适，60 秒是可行的。）

与仅限签名的解决方案的比较

预签名请求中唯一固有的秘密部分是其签名版本 4 签名。 如果客户知道请求的其他详细信息并且获得了与这些详细信息相匹配的有效签名，则它可以发送有效的请求。如果没有有效的签名，则不能。

预签名 URLs 和仅限签名的解决方案在密码学上是相似的。但是，仅限签名的解决方案具有实际优势，例如能够使用 HTTP 标头而不是查询字符串参数来传输签名（请参阅日志交互和缓解措施部分）。 管理员还应考虑到，查询字符串通常被视为元数据，而标头则不太常被当作元数据对待。

另一方面， AWS SDKs 对直接生成和使用签名的支持较少。构建仅限签名的解决方案需要更多的自定义代码。从实际角度来看，为了安全起见，使用库代替自定义代码是一种一般的最佳做法，因此仅限签名的解决方案的代码需要额外的审查。

仅限签名的解决方案不使用`X-Amz-Expires`查询字符串，也没有提供明确的有效期。IAM 管理没有明确到期时间的签名的隐式有效期。那些隐含的时期没有公布。它们通常不会更改，但是在管理时考虑到了安全性，因此您不应该依赖有效期。 在明确控制到期日期和让 IAM 管理到期日之间需要权衡。

作为管理员，您可能更喜欢仅限签名的解决方案。但是，从实际意义上讲，您需要支持已构建的解决方案。

识别预签名的请求

识别使用预签名 URL 的请求

Amazon S3 提供了两种用于在请求级别监控使用情况的内置机制：Amazon S3 服务器访问日志和 AWS CloudTrail 数据事件。 这两种机制都可以识别预签名 URL 的使用情况。

要筛选日志以了解预签名 URL 的使用情况，您可以使用身份验证类型。有关服务器访问日志，请查看 “身份验证类型” 字段，在 Amazon Athena 表中定义该字段时，该字段通常命名为 authty pe。对于 CloudTrail，AuthenticationMethod在`additionalEventData`实地考察。在这两种情况下，使用预签名 URL 的请求的字段值均为`QueryString`，而`AuthHeader`大多数其他请求的字段值均为。

`QueryString`用法并不总是与预签名 URL 相关联。要将搜索限制为仅使用预签名 URL，请查找包含查询字符串参数`X-Amz-Expires`的请求。对于服务器访问日志，请检查 Request-URI 并查找查询字符串中`X-Amz-Expires`包含参数的请求。 对于 CloudTrail，检查`requestParameters`元素中是否有`X-Amz-Expires`元素。

```
{"Records": [{…, "requestParameters": {…, "X-Amz-Expires": "300"}}, …]}
```

以下 Athena 查询将应用此过滤器：

```
SELECT * FROM {athena-table} WHERE
  authtype = 'QueryString' AND
  request_uri LIKE '%X-Amz-Expires=%';
```

对于 AWS CloudTrail Lake，以下查询将应用此过滤器：

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'QueryString' AND
  requestParameters['X-Amz-Expires'] IS NOT NULL
```

识别其他类型的预签名请求

在 Amazon S3 服务器访问日志中`HtmlForm`，POST 请求还具有唯一的身份验证类型，以及 CloudTrail。 这种身份验证类型不太常见，因此在您的环境中可能找不到这些请求。

以下 Athena 查询将过滤器应用于：`HtmlForm`

```
SELECT * FROM {athena-table} WHERE
  authtype = 'HtmlForm';
```

对于 CloudTrail Lake，以下查询将应用过滤器：

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'HtmlForm'
```

识别请求模式

您可以使用上一节中讨论的技术来查找预签名的请求。但是，为了使这些数据有用，你需要找到模式。您的查询的简单TOP 10结果可能会提供见解，但如果这还不够，请使用下表中的分组选项。

分组选项	服务器访问日志	CloudTrail湖	描述
用户代理	`GROUP BY useragent`	`GROUP BY userAgent`	此分组选项可帮助您找到请求的来源和目的。用户代理由用户提供，作为身份验证或授权机制不可靠。但是，如果你正在寻找模式，它可能会揭示很多信息，因为大多数客户使用的是至少部分人类可读的唯一字符串。
请求者	`GROUP BY requester`	`GROUP BY userIdentity['arn']`	此分组选项有助于查找签署请求的 IAM 委托人。如果您的目标是阻止这些请求或为现有请求创建例外，则这些查询可为此目的提供足够的信息。当您按照 IAM 最佳实践使用角色时，该角色会有一个明确标识

分组选项	服务器访问日志	CloudTrail湖	描述
			的所有者，您可以使用该信息来了解更多信息。

分组选项	服务器访问日志	CloudTrail湖	描述
来源 IP 地址	`GROUP BY remoteip`	`GROUP BY sourceIPAddress`	此选项按到达 Amazon S3 之前的最后一个网络转换跳点进行分组。 • 如果流量通过 NAT 网关，则这将是 NAT 网关地址。 • 如果流量通过互联网网关，则这将是将流量发送到互联网网关的公有 IP 地址。 • 如果流量来自外部 AWS，则这将是与来源关联的公共互联网地址。 • 如果它通过网关虚拟私有云 (VPC) 终端节点，则这将是 VPC 中实例的 IP 地址。 • 如果它通过公共虚拟接口 (VIF)，则这将是请求者或任何中介（例如代理服务器或防火墙）仅暴露其 IP 地址的本地 IP。

分组选项	服务器访问日志	CloudTrail湖	描述
			• 如果它通过接口 VPC 终端节点，则可能是 VPC 中实例的 IP 地址。它也可以是来自其他 VPC 或本地网络的 IP 地址。与公共 VIF 一样，这可能是任何中介的 IP 地址。 如果您的目标是实施网络控制，则这些数据非常有用。您可能需要将此选项与诸如`endpoint`（用于服务器访问日志）或`vpcEndpointId`（对于 CloudTrail Lake）之类的数据结合使用以明确来源，因为不同的网络可能会重复私有 IP 地址。
S3 存储桶名称	`GROUP BY bucket_name`	`GROUP BY requestParameters['bucketName']`	此分组选项有助于查找已收到请求的存储桶。这可以帮助您确定是否需要例外。

使用预签名请求的最佳实践

本节讨论安全工程师应考虑的使用预签名请求的最佳实践。这些指导方针包括：

- 基础最佳实践，即每个组织都应遵循的实践。
- 额外的护栏，这是你应该考虑的做法，但可能会决定部分实施或有例外情况实施。它们旨在提供额外的控制和深度防御，但应与整体复杂性保持平衡。
- 记录互动，这可能是由分担责任模式中属于您或您的客户责任一部分的设备或服务引起的。本节包括限制可通过日志访问的信息的预防措施。

基础最佳实践

有效控制其他 AWS API 请求的一般最佳做法也适用于预签名请求。本节回顾了两种最相关的做法：最低权限和数据边界。这些做法创造了其他实践所扩展的控制深度。

采用最低权限原则

限制使用预签名请求的第一步是总体上限制对 Amazon S3 的访问。预签名 URL 无法提供对未授予为预签名 URL 生成签名的委托人的资源的访问权限。它也不能以未授予该委托人的方式提供对资源的访问权限。因此，应用最佳实践来授予这些校长最少的特权是一种有效的保护措施。

创建预签名 URL 的过程是一种基于已发布的签名生成标准（签名版本 4）的算法操作。因此，不可能限制预签名 URL 的生成。但是，为了保持相关性，预签名 URL 必须有效并提供对资源的访问权限，因此预签名 URL 的有效性也是一个有效的保护措施。

有关最低权限的更多信息，请参阅 Fr AWS Well-Architected amework 的 “安全” 支柱中的授予最低权限访问权限。

实现数据边界

最低权限的扩展是维护与组织需求一致的数据边界。预签名 URL 与数据边界兼容。 与其他请求一样，预签名 URL 请求的有效性是在请求时评估的。如果网络、资源、角色会话和主体的属性发生变化，则在接收请求时使用接收请求的方法对其进行评估。

例如，假设在亚马逊 Elastic Kubernetes Service（Amazon EKS）容器中运行的服务签署了请求。该请求随后由连接到互联网的用户的个人计算机系统发送。在本例中，aws: SourceIp 条件评估的是来自用户个人系统的请求的可见公有 IP 地址，而不是 Amazon EKS 容器中服务的 IP 地址。

同样，如果委托人或资源的标签在发送请求之前发生了变化，则更新后的值（不是原始值）将通过 aws: PrincipalTag/tag-key 和 aws: ResourceTag/tag-key 条件应用于请求。

额外的护栏

当解决方案构建者和用户适当地使用预签名的请求时，它们为用户提供了一种安全的数据访问机制。此外，生成预签名请求的功能并不能为委托人提供他们尚未拥有的访问权限。

在这种情况下，是否需要额外的控制措施？ 采取额外控制措施的理由不是基于拒绝访问的需求，而是为了提供监控、批准使用情况和设定界限以及降低用户错误风险的能力。通过这种方式，您可以帮助确保使用是适当和必要的。

以下护栏可帮助您实现这一目标。在启用这些控件之前，您可能需要通过识别预签名的请求来确定现有使用情况。这种识别可以帮助您为护栏对现有使用情况的影响做好准备，或者在需要时计划例外情况。

s3: SignatureAge 的护栏

预签名请求的一个决定性特征是它们描述了过期时间。请求的签名包含日期。对于预签名 URL，此日期作为`X-Amz-Date`查询字符串参数传输，对于预签名 POST，则作为日期或 x-amz-date 标题传输。

Amazon S3 提供了一个名为 s3: SignatureAge 的条件密钥，您可以使用它来限制从签名日期到请求的有效到期之间的最长时间。这种情况永远不会延长有效期，但可以缩短有效期。

在以下策略中，`s3:signatureAge`条件键将预签名请求的有效期限制在 15 分钟以内。以下示例均使用 15 分钟将有效期限制在与标准签名支持的类似时间范围内。

该策略的第二条声明拒绝任何签名版本 2 的访问权限。此版本的签名协议已被弃用，但某些 AWS 区域版本仍受支持。我们建议您在将其完全弃用之前明确屏蔽它。

您可以将以下策略应用为 AWS Organizations 服务控制策略 (SCP)。只要签名生成和使用之间的时间少于 15 分钟，用户仍然可以使用预签名请求并部署依赖于这些请求的解决方案。根据实现的不同，此限制可能不会产生任何影响，也可能导致解决方案无法使用，或者可能导致偶尔出现故障，可以重试。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
```

```
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        }
      }
    },
    {
      "Sid": "DenySignatureVersion2",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
           "s3:signatureversion": "AWS"
        }
      }
    }
  ]
}
```

异常

如果解决方案需要更长的时间才能到期，因此受到上述政策的影响，我们建议您提供一种批准例外情况的方法。为避免枚举 SCP 中的异常，请使用 a ws: PrincipalTag，如以下策略所示，以可扩展的方式管理异常。其他 AWS 示例，例如 AWS 数据边界策略示例，则使用此策略。

如果您通过使用实现异常策略aws:PrincipalTag，则必须控制对委托人设置标签的访问权限。这种类型的标签可以直接来自委托人，也可以由 SCP 控制，如控制可以设置哪些标签值的示例。这种类型的标签也可以来自会话标签，这些标签由身份提供商 (IdP) 设置或在使用时设置。 AWS STS控制访问权限aws:PrincipalTag是一个复杂的话题。但是，具有使用基于属性的访问控制 (ABAC) 经验的组织将具有相应的经验和控制能力，可以aws:PrincipalTag针对此用例进行适当的使用。

在以下示例中，该aws:PrincipalTag条件创建了一个例外，允许分配命名标签 (long-presigned-allowed) 并将其设置为的任何委托人true。除此之外，对签名年龄的限制不适用。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
```

```
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
      }
    }
  ]
}
```

存储桶策略

您可以使用策略将存储桶策略应用于所有或选定的存储桶，如下例所示。与 SCP 不同，存储桶策略还针对服务委托人的使用情况。附录 A 没有记录预签名请求的任何预期服务主体使用情况，但是如果您想实施控制以证明该限制，则以下策略将提供该控制权。此外，与 SCP 不同，存储桶策略可以应用于管理账户中的委托人。

ABAC-based 异常在存储桶策略中的作用方式与 SCP 相同。存储桶政策的目标可能是适用于组织外部的委托人，因此 ABAC 的例外情况应仅限于适用ABAC控制措施的委托人。

在以下示例中，第一条语句中的`aws:PrincipalTag`条件为分配了命名标签 (`long-presigned-allowed`) 且设置为的委托人创建了一个例外`true`。除此之外，对签名年龄的限制不适用。第二条语句将此限制应用于拥有存储桶的 AWS 组织以外的所有委托人。第二条语句的范围应与 ABAC 控件相匹配，以便为委托人设置命名标签。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15MinWithExceptions",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
```

```
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
      }
    },
    {
      "Sid": "DenyPresignedOver15MinutesOutsideOrg",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

资源控制策略

您可以使用资源控制策略 (RCP) 将策略大规模应用于存储桶。与 SCP 一样，与存储桶策略不同，RCP 不以服务委托人的使用为目标。RCP 会影响任何账户的非服务委托人，但不会影响管理账户中的资源。有关详情，请参阅 AWS Organizations 文档。

与存储桶策略一样，如果您使用`aws:PrincipalTags`为委托人创建例外，请记住 ABAC 对委托人标记的控制范围。

以下 RCP 将签名期限限制为 15 分钟，从而限制了组织中所有 S3 存储桶使用预签名 URL。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15MinWithExceptions",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::*/*",
```

```
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true",
        }
      }
    },
    {
      "Sid": "DenyPresignedOver15MinutesOutsideOrg",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::*/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

s3: authType 的护栏

预签名 URL 使用查询字符串身份验证，而预签名 POST 始终使用 P OST 身份验证。Amazon S3 支持通过 s3: authType 条件密钥根据身份验证类型拒绝请求。 `REST-QUERY-STRING`是查询字符串的`s3:authType`值，`POST`也是 POST 的`s3:authType`值。

您可以作为 SCP 应用以下策略。该策略用于仅`s3:authType`允许基于标头的身份验证。它还配置了一种向单个用户或角色提供例外情况的方法。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Action": "s3:*",
```

```
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
}
```

根据身份验证类型拒绝请求会影响使用被拒绝身份验证类型的任何解决方案或功能。例如，拒绝REST-QUERY-STRING会阻止用户从 Amazon S3 控制台进行上传或下载。如果您希望用户使用 Amazon S3 控制台，请不要使用此护栏，也不要将用户作为例外。另一方面，如果您不希望用户使用 Amazon S3 控制台，则可以拒绝REST-QUERY-STRING用户使用。

也许您已经拒绝用户直接访问 Amazon S3 资源。在这种情况下，身份验证类型的护栏是多余的。但是，s3:authType拒绝语句提供了深度防御的效用，因为拒绝直接访问的实现通常跨越许多控制语句，有些则有例外。

用于工作负载的角色通常不需要访问查询字符串或POST身份验证。支持旨在使用预签名请求的服务的角色除外。您可以为这些角色创建特定的例外情况。

您还可以使用诸如以下的策略将存储桶策略应用于所有或选定的存储桶：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
```

```
}
```

此存储桶策略的作用是拒绝使用CopyObject和 UploadPartCopyAPI 制作跨区域副本。Amazon S3 复制不会受到影响，因为它不依赖这些 API。

如果您想使用诸如上述策略之类的存储桶策略，但仍支持跨区域CopyObject或 UploadPartCopyAPI，请添加`aws:ViaAWSService`类似于以下内容的条件：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        },
        "Bool": {
          "aws:ViaAWSService": "false"
        },
      }
    }
  ]
}
```

将预先签名的护栏与其他护栏的例外情况结合起来

如果您不打算对您的用户和角色普遍使用护栏，则可能需要将其应用于其他常见护栏的例外情况，这样这些例外就不支持预签名的请求。

如果您有网络限制，但允许外部合作伙伴例外情况或特殊用例，则应在应用这些例外情况时屏蔽查询字符串或`POST`身份验证，除非明确标识为必填项。

s3: SignatureAge 的局限性

管理员会发现，`s3:signatureAge`更全面地了解其含义很有用。每个已签署的请求都包括`X-Amz-Date`，它应注明当前时间。此值由客户端和请求签名者填写。 AWS 拒绝它认为时间无效的请求。但

是，签名者可以在 future 的时间内提前生成签名。如果请求提前发送得太早，Amazon S3 会拒绝指定未来时间的请求。但是，如果请求直到签名后才发送，则签名可能会更早生成，然后再发送。

`s3:signatureAge`仅对预签名`X-Amz-Date`请求限制签名的最大年限。 超过指定年龄的申请将被拒绝，即使保单到期`X-Amz-Expires`或`POST`保单本来会宣布其有效。 `s3:signatureAge`不会更改不包含明确到期日期的请求的有效期。它也无法控制客户端用于签名的值。`X-Amz-Date`

如果系统时钟错误，或者客户故意将日期设置为未来日期，则签名时间可能不是生成签名的时间。 这限制了解决方案`s3:signatureAge`可以控制的程度。使用生成签名的当前时间的解决方案会受到预期的限制：签名在中指定的毫秒数内保持有效。`s3:signatureAge` 不使用当前时间的解决方案会有不同的限制。一个限制是，用于签署签名的凭证必须仍然有效。作为管理员，您可以控制所颁发的临时证书的最大有效期。 您可以允许证书的有效期最长 36 小时，也可以将有效期限制在 15 分钟以内。 临时证书的到期时间不取决于的值`X-Amz-Date`。

永久凭证没有此限制。 仅使用临时证书是最佳做法，您可以明确撤销任何永久证书，这也会使基于该凭证的所有签名失效。

尽管`s3:signatureAge`以毫秒为单位，但将其设置为小于 60 秒是不切实际的，即使您的时钟同步良好，使用延迟也很低。 低于 60 秒的设置存在拒绝有效请求的风险。如果您预计签名生成和请求提交之间会出现延迟，或者时钟同步出现问题，则应在管理中考虑这些问题`s3:signatureAge`。

大规模定位存储桶

SCP 和 RCP 可以`aws:PrincipalTag`用来为用户设置例外。您不能在存储桶上使用标签来控制访问权限 `aws:ResourceTag` —— 只有对象标签用于访问控制。向要应用此控件的每个对象添加标签通常无法扩展。

适用于许多用例的解决方案是在账户级别应用策略和例外情况，方法是更改 SCP 或 RCP 适用的账户，或者使用 aws: ResourceAccount、aws: 或 a w s: ResourceOrg ID。ResourceOrgPaths例如，可以将 SCP 或 RCP 应用于一组生产帐户。

另一种解决方案是使用自定义 AWS Config 规则来实现侦探控件或响应式控件。目标是让每个存储桶都包含带有适当护栏的存储桶策略。除了测试存储桶策略的内容外，如果存储桶使用特定值标记，则自定义 AWS Config 规则还可以从存储桶中检索标签，并从规则中排除该存储桶。如果该规则未通过合规性检查，则它可以将存储桶标记为不合规，也可以调用补救措施将护栏添加到存储桶的策略中。

> **Note**
>
> 您不能将请求的标签内容限制为PutBucketTagging。要控制存储桶的标记方式，您必须限制对`PutBucketTagging`和的访问权限DeleteBucketTagging。

记录交互和缓解措施

预签名 URL 包含签名，可在到期前的一段时间内用于执行其签名的特定 API 操作。应将其视为临时访问凭证。签名应仅对需要知道的各方保密。在大多数环境中，这是发送请求的客户端和接收请求的服务器。作为直接 HTTPS 会话的一部分发送签名会保持其私有性，因为只有 HTTPS 会话的参与者才能看到传输签名的 URI。

对于预签名 URL，签名作为`X-Amz-Signature`查询字符串参数传输。查询字符串参数是 URI 的组成部分。风险在于客户端可能会用它记录 URI 和签名。客户端可以访问整个 HTTP 请求，并且可以记录请求的任何部分、数据和标头（包括身份验证标头）。但是，按照惯例，这种情况并不常见。URI 日志记录更为常见，在访问日志等情况下是必需的。在记录 URI 之前，客户端应使用密文或屏蔽来删除签名。

在某些环境中，用户允许中介（代理）查看其 HTTPS 会话。启用代理需要对客户端系统的高级特权访问权限，因为它们需要配置和可信证书。在客户端中间环境的本地环境中安装代理配置和可信证书允许非常高的权限级别。为此，应严格控制与此类中介机构的接触。

中介的目的通常是屏蔽不需要的出口，并跟踪其他出口。因此，此类中介机构通常会记录请求。尽管中介机构可以像客户端一样记录任何内容、标题和数据（所有这些都非常敏感），但他们更常见的是记录 URI，例如包含`X-Amz-Signature`查询字符串参数的 URI。

缓解措施

我们建议 URI 日志记录可以删除`X-Amz-Signature`查询字符串参数，编辑整个查询字符串，或者将这些信息视为高度机密信息，就像直接访问中间服务器一样。尽管强烈建议使用这些保护措施，但只要泄露延迟足够长的时间以至于签名到期，预签名 URL 过期这一事实就可以降低日志泄露的风险。

Amazon S3 还会看到签名，并且必须对其进行适当的处理。Amazon S3 服务器访问日志包含请求 URI`X-Amz-Signature`，但建议对其进行编辑。在记录 Amazon S3 CloudTrail 的数据事件时，情况也是如此。 您可以使用自定义数据标识符将 CloudWatch Amazon Logs 配置为屏蔽数据。

以下正则表达式与 URI 中显示的相匹配：`X-Amz-Signature`

```
X-Amz-Signature=[a-f0-9]{64}
```

以下正则表达式添加了分组模式，以更具体地标识要替换的文本：

```
(?:X-Amz-Signature=)([a-f0-9]{64})
```

如果您有如下访问日志条目：

```
X-Amz-Signature=733255ef022bec3f2a8701cd61d4b371f3f28c9f193a1f02279211d48d5193d7
```

第一个正则表达式将访问日志条目转换为：

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

第二个正则表达式在支持非捕获组的系统上，将访问日志条目转换为：

```
X-Amz-Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

常见问题解答

一个预签名的请求可以多次使用吗？ 这是安全风险吗？

是的，预签名请求中的签名可以多次使用。这是否构成安全风险是一个上下文问题。其他访问 AWS 服务的方法也允许重复。具有 AWS 凭据的用户或工作负载可以向发送多个请求 AWS 服务，其中任何一个请求都可能是重复的。

如果您的用例需要执行一次且仅执行一次，则应实施其他机制来强制执行一次性使用。一次性使用不是预签名请求的功能。作为一名安全工程师，您应该查看用例和实现，但在许多情况下，多次使用符合可接受的用途。

目标用户以外的其他人能否使用预签名请求？

预签名请求中的签名可以由任何拥有该签名的人发送。只有当它通过其他形式的验证（例如数据边界控制）时，它才会被接受。如果签名已过期、签名证书已过期，或者签名凭证无法访问所请求的资源，则请求将被拒绝。

其他使用进行身份验证的方法也是如此。 AWS 服务不当共享的凭据允许不当访问。核心最佳做法是仅与目标受众共享凭证和签名。如果您不能相信目标受众会保护私人数据的安全而不与他人共享，那么这将破坏任何形式的身份验证。

授权用户能否使用预签名的请求来泄露数据？

保护数据需要采取强有力的行动。在维护数据边界的同时允许出于预期目的进行访问需要一种全面的方法。 最低权限访问、数据边界控制以及仅使用临时访问凭证是适用于保护数据的一般最佳做法。适当使用这些控件还会限制用户通过他们生成的预签名请求执行操作的能力。

这是因为预签名请求提供的访问权限是授予用于签署请求的凭据的访问权限的子集。在这种情况下，适用于访问数据的最佳做法通常适用于预签名的请求，但是预签名的请求不会创建对数据的新访问权限。

- 最大到期时间仅限于签名证书的到期。 如果签名凭证被撤销，则基于凭证的签名将不再有效。
- 如果与签名证书关联的 IAM 委托人的权限不包括执行与预签名请求相关的操作，则调用预签名请求会导致 “访问被拒绝” 响应。 响应取决于调用时权限的当前状态，这与生成预签名请求签名的时间无关。

- 委托人的属性是根据与签名凭证关联的委托人进行评估的。
- 根据与签名凭证关联的角色会话来评估角色会话的@@ 属性。
- 与普通请求一样，网络的属性是根据请求的接收方式来评估的。

在这种情况下，对与预签名请求相关的风险的审查仅限于使用与用户凭证不同的凭据签署的区域，并且提供的访问权限不是用户主体的一部分。此检查应应用于服务设计、工作负载或代表用户生成签名的解决方案，而不是预签名的请求功能本身。

如果我怀疑预签名 URL 是以未经授权的方式共享的，我能否拒绝该网址的访问？

可以。这需要使 URL 签名时使用的凭据失效。有多种方法可以做到这一点：

- 移除证书所属的 IAM 委托人的权限。如果该 IAM 委托人不再有权访问该 URL 所签名的资源和操作，则该 URL 将无法执行该操作。这会影响该 IAM 委托人的所有匹配使用。
- 如果用于签名 URL 的证书是临时 AWS STS 证书，则可以撤消在特定时间之前为 IAM 委托人颁发的临时证书的会话权限。根据用例，可能还有其他有效会话在正常到期时间之前失效，但新会话不会受到影响。撤消会话权限也会使使用与这些会话关联的凭证签署的任何 URLs 权限失效，但是与新会话 URLs 关联的新会话不会受到影响。
- 如果用于签名 URL 的凭证是永久凭证，请停用访问密钥。这会影响与这些凭证相关的所有用法。

资源

Amazon S3 文档

- 对@@ 请求进行身份验证（AWS 签名版本 4）
- 对@@ 请求进行身份验证：使用查询参数（AWS 签名版本 4）
- 对@@ 请求进行身份验证：使用 POST 进行基于浏览器的上传（AWS 签名版本 4）
- Amazon S3 签名版本 4 身份验证特定策略密钥
- 使用预签名 URL

其他参考资料

- 在 AWS 上构建数据边界（AWS 白皮书）
- SEC03-BP02 授予最低权限访问权限（架构AWS 良好的框架，安全支柱）
- SEC03-BP05 为您的组织定义权限护栏（架构AWS 良好的框架、安全支柱）

附录 A：如何 AWS 服务 使用预签名 URLs

本附录提供有关使用预签名的 AWS 服务 URLs信息和功能。此信息有两个用途：

- 为实施控制措施的安全工程师提供有关这些控制措施可能产生的影响的信息。
- 让人们意识到这种风险可能与网址记录交互相关的情况。

> **Important**
>
> 本附录未提供预签名的 URLs完整列表 AWS 服务 或其用法。它也不涵盖定制解决方案或第三方解决方案。

Amazon S3 控制台

主体：控制台用户

默认到期时间：5 分钟

> **免责声明**
>
> 本节记录了 Amazon S3 控制台的当前行为。 AWS 控制台行为如有更改，恕不另行通知。

Amazon S3 控制台支持下载和上传对象。 下载使用过期时间为 300 秒（5 分钟）的预签名 URL。 URL 是由向的请求生成的`https://<bucket-region>.console.aws.amazon.com/s3/batchOpsServlet-proxy`。

该请求是在用户点击下载按钮时启动的，因此在出现明确的下载请求之前，URL 不会提前生成或发送给客户端。

上传内容类似，唯一的不同是控制台发送两个请求：`OPTIONS`作为飞行前 CORS 检查，以及。PUT 两个请求都使用相同的签名。

用于签名的凭证是与当前登录的用户关联的临时证书。 有关获取这些临时证书的方法的详细信息不在本指南的讨论范围之内。

Amazon S3 Object Lambda

负责人：接入点呼叫者

默认过期时间：61 秒

> **Note**
>
> 自 2025 年 11 月 7 日起，S3 Object Lambda 仅适用于当前正在使用该服务的现有客户以及精选 AWS Partner Network (APN) 合作伙伴。要了解与 S3 对象 Lambda 类似的功能，请在此处了解更多信息 — Amazon S3 对象 Lambda 可用性变更。

Amazon S3 对象 Lambda 使用 AWS Lambda 函数自动处理和转换从亚马逊 S3 检索的数据。当 S3 Object Lambda 调用函数时，会为该函数提供一个预签名 URL (`inputS3Url`)，它可以使用该网址从支持的接入点下载原始对象。

这些预签名 URLs 是为支持的 Amazon S3 接入点签名的，该接入点是在您配置 S3 对象 Lambda 时提供的。（这与对象 Lambda 接入点不同。）与其使用绑定到 Lambda 函数的角色，不如使用原始调用者的身份签名 URL，并且该用户的权限将在使用该 URL 时生效。如果 URL 中有已签名的标头，则 Lambda 函数必须在对 Amazon S3 的调用中包含这些标头。

返回的预签名 URL 的过期时间为 61 秒（比 S3 对象 Lambda 函数的最大持续时间多一秒）。生成的 URL 只能与支持的接入点一起使用。S3 对象 Lambda 接入点的调用者需要有权访问该接入点。您可以使用条件限制对 S3 对象 Lambda 上下文的访问权限。`"aws:CalledVia": ["s3-object-lambda.amazonaws.com"]`当该条件附加到支持的接入点或存储桶时，用户无法直接访问支持的接入点或存储桶。

这种方法的价值在于，无需向 Lambda 函数授予对您的 S3 存储桶或访问点的访问权限。与 Lambda 函数关联的角色需要权限 WriteGetObjectResponse，但不需要权限。GetObject

当 S3 对象 Lambda 生成预签名时 URLs，它不会添加网络限制，因此可以在 Lambda 函数之外使用网址。但是，对 S3 对象 Lambda 的调用者施加的任何限制仍然适用。例如，如果您的 Lambda 函数在 VPC 中运行，并且您限制调用者只能使用 VPC 终端节点，那么任何拥有预签名 URL 的人都需要能够通过该 VPC 终端节点发送它。 此限制也适用于SourceIp和VpcSourceIp。

> **Note**
>
> 要在 VPC 中使用 S3 对象 Lambda 函数，VPC 必须有通往公有 S3 终端节点的路由才能调用。WriteGetObjectResponse 这并不表示使用 VPC 终端节点的要求不适用于从存储桶检索数据的请求。

AWS Lambda 跨区域 CopyObject

校长：AWS 内部

默认到期时间：3600 秒

当您使用CopyObject或 UploadPartCopyAPI 进行复制时 AWS 区域，Amazon S3 在 URLs内部使用预签名。它们 APIs 可以直接从命令中调用， SDKs 也可以从 AWS CLI 命令`aws s3api copy-object`和中调用`aws s3api upload-part`。它们 APIs 不用于 Amazon S3 复制，但是当源 AWS CLI `aws s3 cp`和目标是 S3 存储桶时，和`aws s3 sync`命令会使用它们。它们还得到各种`TransferManager`实现的支持 AWS SDKs。

AWS Lambda GetFunction

校长： AWS 内部

默认到期时间：10 分钟

AWS Lambda 在生成部署到 Lambda 容器的资产之前，将用户版本存储在 Lambda 团队拥有的 S3 存储桶中。 当你想访问函数的代码时，你可以调用 GetFunctionAPI。 此 API 的响应为`Code.Location`，其中包含一个有效期为 10 分钟的预签名 URL（此到期时间是当前行为，不是已发布的合同）。 如果您不想要代码，则可以使用GetFunctionConfigurationGetFunctionConcurrency、和的组合ListTags来检索返回的其他数据`GetFunction`。

返回的 URL 不是使用当前登录用户的证书签名的，而是由 Lambda 代表用户签名的。因此，应用于当前登录的用户或该用户的临时会话凭证的条件密钥（例如`aws:SourceIP`）不适用于生成的 URL。无论条件密钥GetFunction仅应用于用户或会话的所有 AWS API 使用情况，还是应用于该用户或会话的所有 AWS API 使用情况，都是如此。

Lambda 控制台还使用它返回GetFunction的预签名 URL。 控制台使用与当前登录用户关联的临时凭证进行呼叫GetFunction。有关获取这些临时证书的详细信息不在本文档的讨论范围之内。

Amazon ECR

校长： AWS 内部

默认到期时间：1 小时

Amazon Elastic Container Registry (Amazon ECR) 提供GetDownloadUrlForLayer了 API，它返回一个有效期为一小时的预签名 URL，并支持从亚马逊 ECR 图像下载单个图层。但是，此操作由 Amazon ECR 代理使用，用户通常不使用此操作来拉取和推送图像。

Amazon Redshift Spectrum

主体：角色通过传递给创建外部架构 `IAM_ROLE`

默认到期时间：1 小时

Amazon Redshift Spectrum 在内部使用 URLs 预签名，禁止限制存储桶和亚马逊 Redshift 角色的组合，以限制预签名。 URLs 您可以使用 16 分钟的`s3:signatureAge`值，但值过低是不可靠的。您可以使用的最小值取决于查询的时间和大小。尽管小于 16 分钟的值适用于许多场景，但它需要测试。可以而且应该将该角色限制为仅供Redshift Spectrum使用，而Redshift Spectrum不会透露 URLs 其生成的内容，从而减轻了降低过期值的典型理由。

亚马逊 A SageMaker I Studio

亚马逊 SageMaker AI Studio 支持两个 API 操作：CreatePresignedDomainUrl和CreatePresignedNotebookInstanceUrl。但是，这些 APIs 与签名版本 4 的预签名 URL 功能无关。它们会 APIs 创建一个使用`authToken`参数的 URL，但它们不支持任何标准的 Signature 版本 4 查询参数。

`authToken`是一种不同的机制，但与预签名 URLs有相似之处。它作为查询字符串参数发送，并支持 5 分钟的过期时间。

SageMaker AI 支持网络限制。如果您对操作设置了限制，则该`sagemaker:CreatePresignedDomainUrl`操作既适用于调用 CreatePresignedDomainUrl，也适用于生成的 URL 的使用。如果 URL 是从有效的网络生成的，然后由无效的网络发送，则生成网址的 API 调用会成功，但是发送网址的请求会失败。`sagemaker:CreatePresignedNotebookInstanceUrl`动作也是如此。CreatePresignedNotebookInstanceUrl

有关更多信息，请参阅 A SageMaker I 文档。

附录 B：预签名的 URLs 控件如何影响 AWS 服务

本附录描述了使用预签名的 URLs控件（如附录 A 中所述）与本指南前面描述的控件之间的交互。AWS 服务

s3: SignatureAge 的护栏

Amazon S3 控制台不会因为`s3:signatureAge`条件密钥设置的最长 5 分钟到期时间而中断。 当您选择 “下载” 按钮 URLs 时，Amazon S3 控制台会生成预签名，并应用自己的 5 分钟到期时间。短于 2 分钟的最大持续时间可能会导致基于时钟同步和延迟的随机故障。

Amazon S3 Object Lambda 使用的过期时间为 61 秒，因此将条件设置`s3:signatureAge`为 61 秒或更长时间不会造成任何中断。较短的持续时间可能不太可靠，并可能导致间歇性故障。

Amazon S3 跨区域CopyObject不会因为最长 5 分钟的过期时间而中断。但是，较短的持续时间可能会导致基于时钟同步和延迟的随机故障。

在中 AWS Lambda，GetFunction提供指向客户账户之外对象的 URL，因此客户政策不会影响生成的对象 URLs。

亚马逊 Redshift Spectrum 已经过测试`s3:signatureAge`，条件为 16 分钟。但是，较短的持续时间可能会导致中断。

不使用网络限制时 s3: authType 的护栏

Amazon S3 控制台通常会受到`s3:authType`护栏的影响。 控制台根据本地网络配置路由到 Amazon S3。 如果本地网络以网络限制允许的方式路由到 Amazon S3，则 Amazon S3 控制台仍然可以运行。但是，如果以不允许的方式通过代理或公共互联网进行路由，则使用将被阻止。 但是，阻止使用可能是该政策的目的。

如果 Lambda 函数未连接到相应的 VPC，则 Amazon S3 对象 Lambda 会受到影响。 在此配置中，VPC 必须具有 NAT 网关，不是为了访问 S3 存储桶，而是为了调用WriteGetObjectResponse。

如果将此保护措施应用于存储桶策略，而没有建议的例外情况（何时**`aws:viaAWSService`**为真），则会中断 Amazon S3 跨区域CopyObject。

除非使用增强型 VPC 路由`s3:authType`，否则 Amazon Redshift Spectrum 会受到护栏的影响。目前，Redshift Spectrum 仅支持无服务器集群的增强型 VPC 路由，不支持已配置集群的增强型 VPC 路由。

文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 RSS 源。

变更	说明	日期
更新和澄清	在“其他护栏”部分，添加了有关例外情况的信息 RCPs 并对其进行了澄清。	2025 年 8 月 8 日
初次发布	—	2024 年 7 月 23 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。